

# REDDOXX

**User Manual**  
for  
the User Console,  
the Outlook AddIn  
and the Web Interface

Version 1027

[www.reddoxx.com](http://www.reddoxx.com)

## Copyright

©2009 by REDDOXX GmbH

### **REDDOXX GmbH**

Saline 29  
D-78628 Rottweil

Fon: +49 (0)741 248 810  
Fax: +49 (0)741 248 811

Email: [info@reddox.com](mailto:info@reddox.com)  
Internet: <http://www.reddox.com>  
Support: <http://support.reddox.net>

Revision number: 2.44

Last alteration: 21.1.2010

This manual was prepared with great care. However, REDDOXX GmbH and the author cannot assume any legal or other liability for possible errors and their consequences.

No responsibility is taken for the details contained in this manual. Subject to alternation without notice. REDDOXX GmbH does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement.

This manual is protected by copyright law. REDDOXX GmbH reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of REDDOXX GmbH. The latter especially applies for data processing systems.

REDDOXX GmbH also reserves all communication rights (lectures, radio and television).

The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of REDDOXX GmbH.

This issue replaces all earlier ones and orients itself on the appliance with respect to naming.

## Table of contents

1	Introduction and Start .....	4
1.1	REDDOXX User Console.....	4
1.2	REDDOXX Outlook Add-In.....	4
1.3	REDDOXX Web Interface.....	4
2	Login.....	5
2.1	Login with the User Console .....	5
2.2	Login within MS Outlook.....	5
2.3	The welcome screen .....	7
3	Options in the menu bar .....	8
3.1	Outgoing Mails.....	9
3.2	Spam Mails.....	10
3.2.1	Spam Mail Options .....	10
3.3	CISS queue .....	11
3.4	Archive.....	12
3.4.1	Archive Search .....	12
3.4.2	Archive options.....	16
3.5	MailSealer.....	19
3.6	User Settings.....	20
3.6.1	User Profile.....	21
3.6.2	E-Mail Aliases .....	22
3.6.3	Filter lists.....	24
3.7	Logoff.....	26
4	The Reddoxx Outlook AddIn.....	27
4.1	Installation of the Outlook AddIn .....	27
4.2	Outlook menu overview .....	30
4.3	Reddoxx logon.....	30
4.4	The Reddoxx menu .....	31
4.5	Message archiving.....	31
4.6	Blacklisting an email manually .....	34
5	Glossary .....	36

# 1 Introduction and Start

For maintaining the Reddoxx Appliance there are several user interfaces to your choice.

1. REDDOXX User Console
2. REDDOXX Outlook Add-In
3. REDDOXX Web Interface

All this solutions gives you nearly the same function set and a consistently Look & Feel. Some variations will be marked in the corresponding chapter of this user manual with a symbol and described.

## 1.1 REDDOXX User Console



Die REDDOXX User Console is a portable program file with the extension named <.exe>. It will not be installed but executed with a double click directly. This software can be downloaded from the REDDOXX Support Center. There is also a <.msi> version to distribute it into the network.

## 1.2 REDDOXX Outlook Add-In



Das REDDOXX Outlook-AddIn is a Windows-DLL which is integrated into Microsoft Outlook with the AddIn technology. The AddIn is loaded within the start up of Outlook. If a REDDOXX specific function is used for the first time after loading Outlook, a login is required. The AddIn only supports Outlook version 2002 - 2007 and only in combination with MS Exchange Server. The Installation and some special features of the Outlook-AddIn are described at the end of this document in chapter 4. Outlook 2000 work fine in principe just with little restrictions in the context menu of a mail but is not supported by REDDOXX.

## 1.3 REDDOXX Web Interface



The REDDOXX Web Interface (WI) is provided by the Appliance itself. You only need a common web browser to access your emails. Insert following address into your browser:

**http://<IP-Adresse-oder-Hostname-der-Appliance>**

**https://<IP-Adresse-oder-Hostname-der-Appliance>** (encrypted)

## 2 Login

For safety reasons, the REDDOXX Appliance is only accessible via login. Therefore you have to authenticate yourself as follows with your user name and password.

### HINWEIS

The Purchase of a REDDOXX Appliance with valid licenses is required



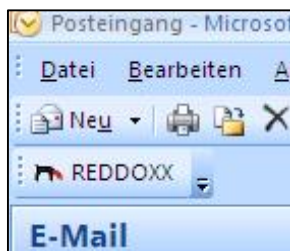
## 2.1 Login with the User Console

1. Double-click on the file rdxuser.exe.  
The login window appears. Continue with step 3 at the login window.



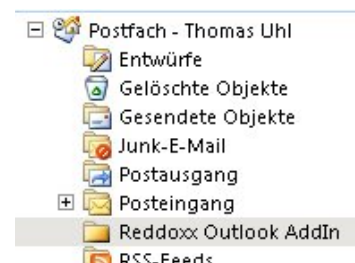
## 2.2 Login within MS Outlook

1. Launch MS Outlook.



In the tool bar now a Reddoxx button is shown. Additionally you've got a new folder below your post box named *Reddoxx Outlook AddIn*.

Illustration: Reddoxx button and Reddoxx folder



2. Click onto the Reddoxx button or click onto the Reddoxx Outlook AddIn folder to log in.

The log in window appears.

## The Login window

The software automatically searches for existing Appliances inside your local network. In the field „**Appliance found**“ all automatically detected Appliances are listed.

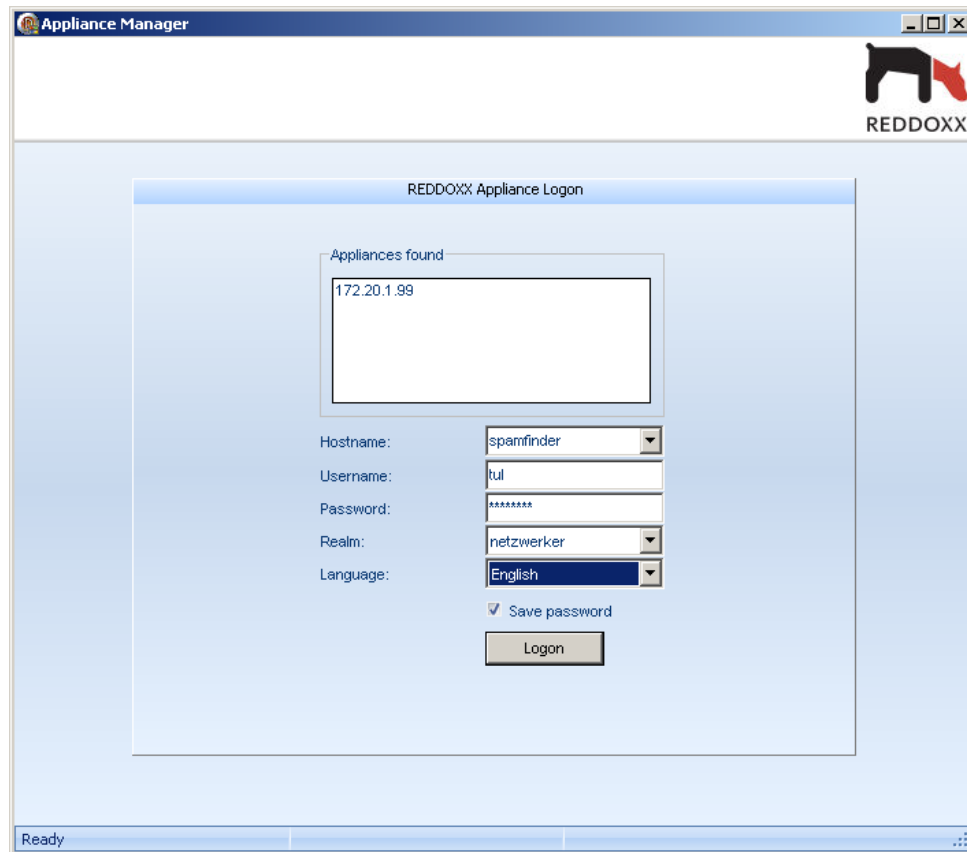


Illustration: LogIn window

3. **Hostname:** Choose the hostname or IP address from the field „Appliance found“ with a double click so that will be inserted automatically into the field “hostname”. You also can insert manually a hostname or an IP address of your Appliance into this field. (contact your administrator if you don't know it).
4. **Username:** Enter your user name.
5. **Password:** Enter your password.
6. **Realm:** select the option „local“ or the realm which you belong to. The realm is a section similar to a domain in which you have to authenticate yourself.
7. **Language:** Choose the desired language in the selection list. The selection contains the currently installed languages German, English, Italian and Dutch.
8. **Save Password:** The password will be kept for the next login to enable auto login.
9. **Logon:** Click on the button LOGON. Continue with the welcome screen.

## 2.3 The welcome screen

The welcome screen after a successful login.

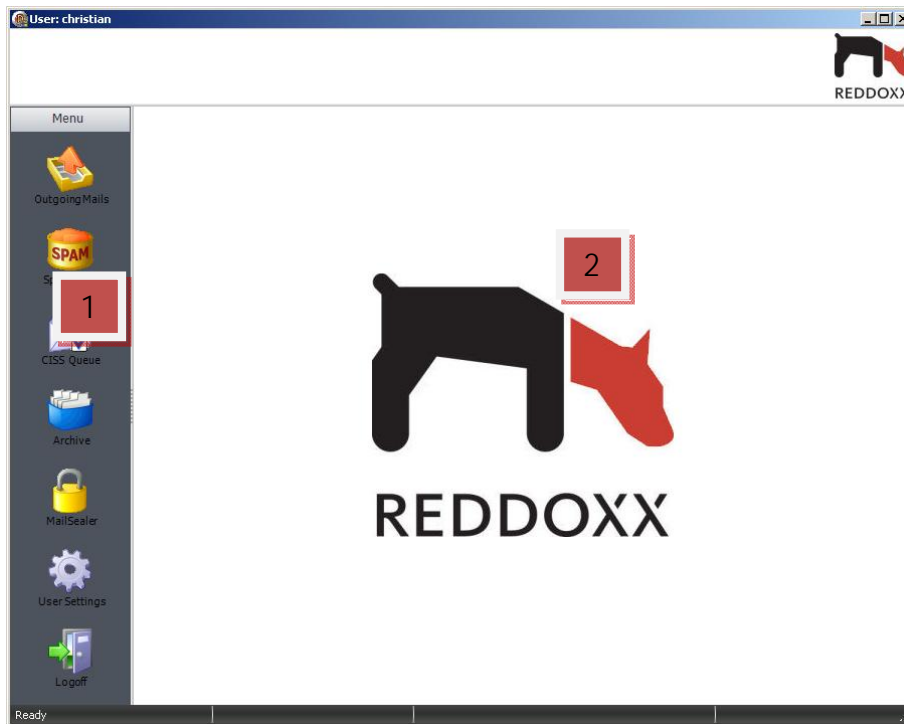


Illustration: Application window after login

**Legend:** 1. Menu bar, 2. Display window.

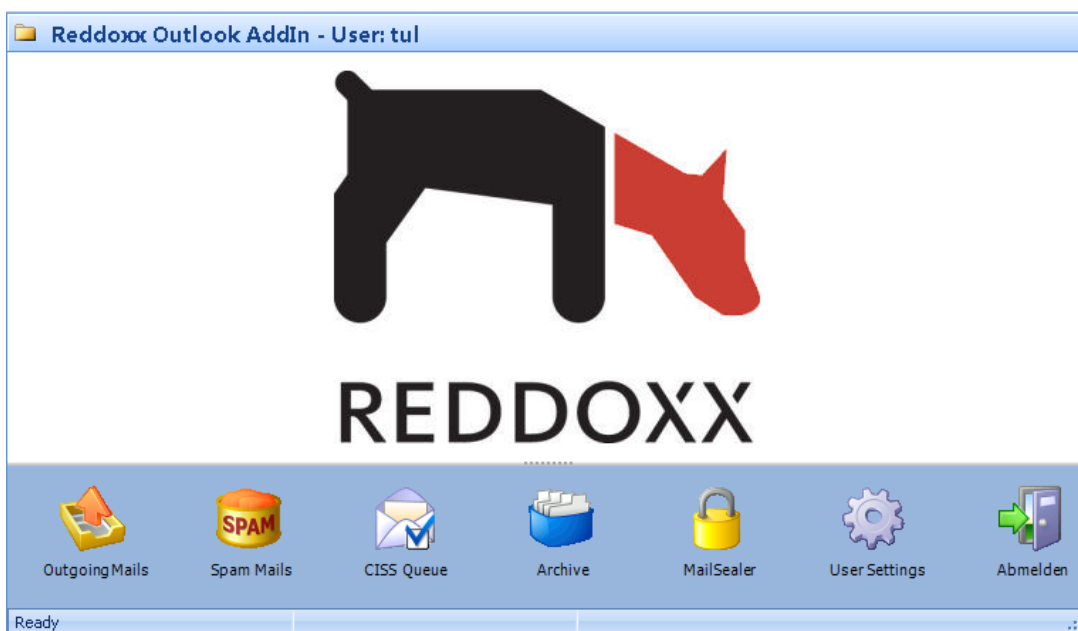
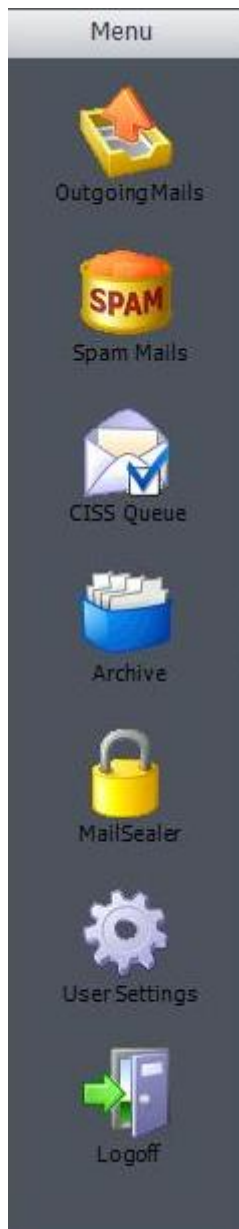


Illustration: Application window after login within MS Outlook

### 3 Options in the menu bar

The main menu consists of Outgoing mails, Spam, CISS queue, Archive, Mail Sealer, User settings and Logoff.



#### **Outgoing Mails**

Here you get all emails listed that the user is sending to the internet.

#### **Spam Mails**

Here are listed all mails that were sent to the user but were detected as spam.

#### **CISS Queue**

The CISS Queue contains all emails which has been kept back and has not been released yet by the sender or by the recipient.

#### **Archive**

In the Mail Depot you will find all the emails which have been archived by the appliance.

#### **Mail Sealer**

The Mail Sealer (Light) offers you the possibility to send your email encrypted with a password.

#### **User Settings**

The user settings allow you to change your general setting. You can maintain your email addresses here.

#### **Logoff**

You log off from your personal user GUI.

Illustration: Menu bar



## 3.1 Outgoing Mails



All e-mails scheduled to being sent by the Appliance will first be put into the Outgoing E-Mails Queue. The Outgoing Mails section lists all of these e-mails.

If the e-mail could not have been sent immediately due to a failure at the recipient's side or to a network failure, your Appliance attempts to send the e-mail again in regular intervals. After approximately 1.5 hours delay the sender receives a first notification that the e-mail could not have been delivered up to now.

The '*Last Result*' column informs you about the cause of the failure.

If the failure is removed but you do not want to wait for the next sending cycle you can instantly send the respective e-mail by making a right click on it. It is possible to select various e-mails at once.

If the delivery of the e-mail should not be possible permanently, because of mistyping in the domain name of the e-mail address, for instance, you can delete the e-mail by making a right click on it. However, an e-mail which cannot be delivered within a period of 5 days will be deleted automatically from the Outgoing E-Mails Queue. The sender receives a notification about this event.

Outgoing Mails

Find:

in

Sender

Search

Queue:

SMTP


ID	Received	Sender	Recipient	Size	Delivery time	Last result
 7DD8B6B7B...	01.12.2009 16:37...	tul@netz...	dfgdj@dgdhfgdj....	9,11 KB	04.12.2009 06...	No mail server found for domain: dgdhfgdj....

Image: Outgoing E-Mails

**Find:** You can search for specific e-mails across the Outgoing E-Mails Queue as well as to delete e-mails that are listed there. In the list view you can see the ID, the time the e-mails has been received, the sender of the e-mail, its recipient and the size of the e-mail. You can also sort the e-mails by their criteria here. To do so please click on the column heading.

**In:** Restrict the search by either searching for the *sender* or the *recipient* of the e-mail.

**Queue:** You can choose between **SMTP** and **POP3**.

In the **SMTP Queue** there are e-mails which have not been sent yet. In the **POP3 Queue** there are e-mails which have already been collected from the inboxes but have not yet been validated by the Box. The e-mails are then waiting for the next retrieval through the e-mail client program.

## 3.2 Spam Mails



E-mails that are listed in the Spam Mails Queue have been classified as spam by the Appliance. In case e-mails should have been recognized as spam accidentally (False Positive) you can deliver them to the recipient manually afterwards.

Spam Mails

Find:

in

Sender

Search

Deputy:

None







ID	Received	Sender	Recipient	Size	Subject	Filter
 1E5FFF64425	04.12.2009 06:3...	stephont@aeromundoviaje...	tul@netzw...	7,89 KB	email that his	Fuzzy-Filter
 79F996BA5F7	04.12.2009 04:2...	robert_maryjosa@aditamil...	tul@netzw...	2,08 KB	"Buy CializViagr...	Fuzzy-Filter
 825F84956B2	04.12.2009 00:1...	tuyetkrysta_xr@ndtv.com	tul@netzw...	1,95 KB	iRo1exRep1ica ...	Fuzzy-Filter
 284C73BF403	03.12.2009 12:2...	shelleychapman@kichimail....	tul@netzw...	2,33 KB	Die modischen ...	Fuzzy-Filter
 71BF79C8C...	03.12.2009 07:3...	8yg30@tanisc.com	tul@netzw...	1,34 KB	Ihrem Konto wur...	Fuzzy-Filter
 1DF2C7D1...	03.12.2009 00:5...	opalkaiser@edomex.com	tul@netzw...	1,41 KB	Der beste Preis ...	Fuzzy-Filter

Image: Spam Mails

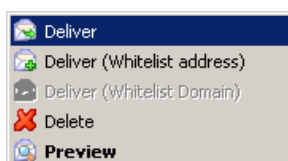
**Find:** You can search for specific e-mails across the Spam Mails Queue as well as to delete e-mails that are listed there. In the list view you can see the ID, the time the e-mail has been received, the sender of the e-mail, its recipient and the size of the e-mail. You can also sort the e-mails by their criteria, here. To do so please click on the column heading.

**In:** Restrict the search by either searching for the *sender* or the *recipient* of the e-mail.

**Deputy:** Please select the e-mail address whose queue you are allowed to manage as a deputy from the deputy list. Via the *Settings* section you can determine a deputy who is supposed to substitute your own queues then.

### 3.2.1 Spam Mail Options

You have certain options to process the spam mail afterwards. Make a right click on a selected spam mail to open the context menu.



**Deliver:**

The mail will be delivered immediately.

### Deliver (Whitelist Address):

The mail will be delivered immediately and added to address white list.

### Deliver (Whitelist Domain):

The mail will be delivered immediately and the sender's domain name will be added to domain white list.

### Delete

Spam mails are being deleted automatically from the Spam Mails Queue after a period of 60 days. However, you can manually delete specific or multiple emails from the queue anyway. To do so make a right click on the e-mail you want to delete and select the '*Delete*' option from the context menu.

### Preview

The preview of your emails allows you to have a first look on your spam mails before you decide to have them either delivered or deleted.

## 3.3 CISS queue



When using the CISS filter the sender receives an email which must be acknowledged, so that his email to you will be sent. The mail remains in the CISS queue until it will be confirmed. You can browse the CISS queue if you wait for a certain mail and you can bypass the filter permanently for the senders address.

CISS Queue

Find:  in

Deputy:


ID	Received	Sender	Recipient	Size	Subject
 834E6307438	01.12.2009 17:32:46	thomas@thomasuh...	tul@netzwer...	6,76 KB	test

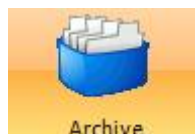
Illustration: Search CISS queue

The search, deliver, delete and preview options are consistent with those of the spam mails.

### NOTICE

E-Mails (e.g. newsletters) which have not been confirmed by the sender can be released by yourself.

## 3.4 Archive



Within the archive there are all e-mails stored that have been sent or received by the Appliance. You can display a list of all your e-mails as well as you can deliver specific e-mails to your mail box again. You can also search for specific e-mails by specifying certain criteria.

Archive search

Find:  In:

Deputy:

[advanced search](#)

[advanced full text search](#)

ID	Message time	Subject	Sender	Recipient	Size
00000...	18.08.2009 11:51:32	test easy			482 Byte
00000...	18.08.2009 11:35:40	reddoxx			5,38 KB
00000...	18.08.2009 11:28:31	test reddoxx			5,45 KB

Image: Archive

### 3.4.1 Archive Search

For the search within the archive there are three different search procedures available:

- The Simple Search (including full text search)
- The Advanced Search
- The Advanced Full Text Search

#### NOTICE

Following file formats are supported for full text indexing:  
MS Office until Office 2003, PDF and text files (with extension .txt).

Please also note, that embedded images inside a PDF document, as for e.g. a facsimile, currently can not be retrieved from the full text search.

### 3.4.1.1 The Simple Search (with full text search)



Image: Default Archive Search

**Find:** One or multiple search patterns that all must exist in the searched content. (Boolean AND). Wild cards (e.g. “\*”) are not permitted.

**In:** Choose one of the following content type.

*Full text:* The content type *Full text* is the default. The full text search searches in the whole email for those specified search patterns. The search consists of the complete archive without any temporal restrictions. The full text search also includes the content of the attachments. Supported attachment types are currently MS Office until 2003, TXT-Files and PDF-documents. The indexing of the new emails of a day starts at 22:00h per default. Please note that emails of the current day can not be found with the full text search until the indexing has finished. In this case, use the advanced search.

*Sender:* Searches for the sender of an email.

*Recipient:* Searches for the recipient of an email.

*Subject:* Searches for the subject of an email.

*Sender and Recipient:*

Searches for the sender or for the recipient. If the searched pattern is in one of these fields, the email is shown in the result list.

*Attachments:* Searches only in the file name of the attachments. Do not confuse this issue with the searching in the content of an attachment. This can only be done by the full text search.

#### NOTICE

Searching with other content type than full text, is limited by the time range, defined in the appliance configuration option called “default display period”. The default is 30 days back.

Our recommendation:

Prefer the simple full text search, if you do not need to look for emails of the current day.

## Deputy:

Selecting „*none*“ shows only emails matching the from or to field. If you are looking for emails which you are deputising, you need to select the relevant email address from this drop down box.

### 3.4.1.2 Advanced Search

Using the advanced search you can combine various search criteria with each other and limit specified time period, but a full test search is not supported.

Image: Advanced Archive Search

- From Date: / To Date:** Restrict the search by specifying a period of time.
- Use archiving date:** Not the sending date but the archiving date will be respected for the search. Please note that the date, and particularly the time, between the creation and the receiving of the e-mail can diverge from each other significantly.
- E-mail address:** Search for the email address of the sender or the recipient. Adjust the corresponding setting in the subsequent field on the right. ‘*Sender and Recipient*’ means: either – or.
- Subject:** Specify a part of the subject you are searching for. Wildcards (like \*) and regular expressions are not allowed here.
- Attachment:** Specify a part of the attachments filename you are searching for. Please note that the name of the file will be searched and not it’s content (see full text search).
- Deputy:** Selecting „*none*“ shows only emails matching the from or to field. If you are looking for emails which you are deputising, you need to select the relevant email address from this drop down box.

- Include Spam Mails:** Perhaps an email was marked as spam accidentally (false positive). With this option you can also search for spams inside the archive but only if archiving spam not been disabled (ask your administrator). Also emails which have been put into the CISS queue are treated as spam and need to have this option enabled, if you want to include it into your search.
- Include Virus Mails:** Perhaps, as like spam, an email was filtered because of a virus. With this enabled option, the email is included to the search criteria. Otherwise it is hidden to the search.

### 3.4.1.3 Advanced full text search

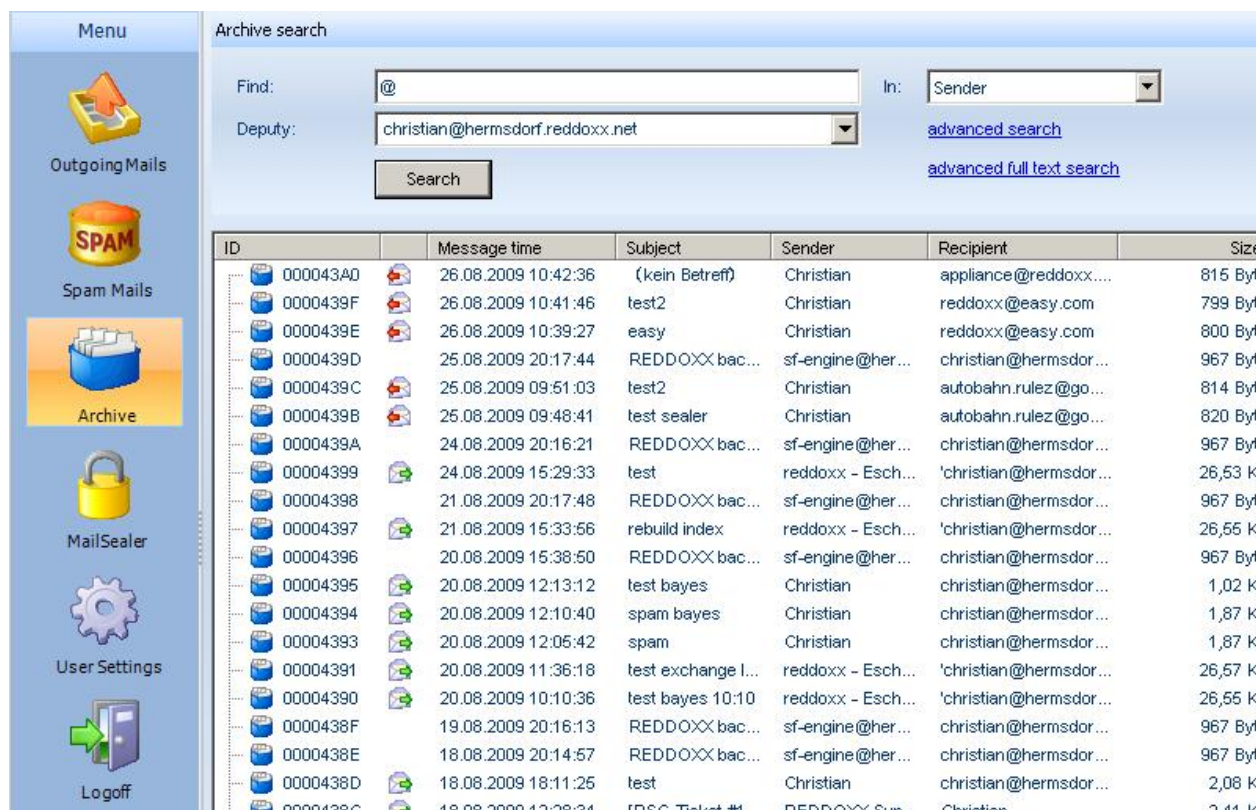
In the advanced full text search you can combine various search terms with each other logically. As in the simple full text search the content of the file attachment will be searched as well. Wildcards (like \*) and regular expressions are not allowed here either. The advanced full text search is not available in the web interface currently.

Image: Advanced Full Text Search

- All of the words:** All of the words specified need to occur in the e-mail you was searching for.
- At least one of the words:** At least one of the words specified needs to occur in the e-mail you were searching for.
- Without the words:** The word specified must not occur in the e-mail you were searching for.
- Deputy:** Selecting „none“ shows only emails matching the from or to field. If you are looking for emails which you are deputising, you need to select the relevant email address from this drop down box.



## Archive Search showing search results:



Archive search

Find:  In:   
 Deputy:  [advanced search](#)  
[advanced full text search](#)

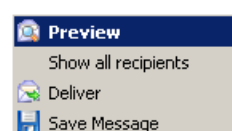
Search

ID	Message time	Subject	Sender	Recipient	Size
000043A0	26.08.2009 10:42:36	(kein Betreff)	Christian	appliance@reddox...	815 Byt
0000439F	26.08.2009 10:41:46	test2	Christian	reddox@easy.com	799 Byt
0000439E	26.08.2009 10:39:27	easy	Christian	reddox@easy.com	800 Byt
0000439D	25.08.2009 20:17:44	REDDOXX bac...	sf-engine@her...	christian@hermsdor...	967 Byt
0000439C	25.08.2009 09:51:03	test2	Christian	autobahn.rulez@go...	814 Byt
0000439B	25.08.2009 09:48:41	test sealer	Christian	autobahn.rulez@go...	820 Byt
0000439A	24.08.2009 20:16:21	REDDOXX bac...	sf-engine@her...	christian@hermsdor...	967 Byt
00004399	24.08.2009 15:29:33	test	reddox - Esch...	'christian@hermsdor...	26,53 K
00004398	21.08.2009 20:17:48	REDDOXX bac...	sf-engine@her...	christian@hermsdor...	967 Byt
00004397	21.08.2009 15:33:56	rebuild index	reddox - Esch...	'christian@hermsdor...	26,56 K
00004396	20.08.2009 15:38:50	REDDOXX bac...	sf-engine@her...	christian@hermsdor...	967 Byt
00004395	20.08.2009 12:13:12	test bayes	Christian	christian@hermsdor...	1,02 K
00004394	20.08.2009 12:10:40	spam bayes	Christian	christian@hermsdor...	1,87 K
00004393	20.08.2009 12:05:42	spam	Christian	christian@hermsdor...	1,87 K
00004391	20.08.2009 11:36:18	test exchange l...	reddox - Esch...	'christian@hermsdor...	26,57 K
00004390	20.08.2009 10:10:36	test bayes 10:10	reddox - Esch...	'christian@hermsdor...	26,56 K
0000438F	19.08.2009 20:16:13	REDDOXX bac...	sf-engine@her...	christian@hermsdor...	967 Byt
0000438E	18.08.2009 20:14:57	REDDOXX bac...	sf-engine@her...	christian@hermsdor...	967 Byt
0000438D	18.08.2009 18:11:25	test	Christian	christian@hermsdor...	2,08 K

Image: Archive Search showing Search Results.

## 3.4.2 Archive options

Various manual options are in the individual processing of those messages available. By clicking the right mouse button on the display the following options appears.



### Preview:

The contents of the email will be displayed in a separate window. For example:

### Deliver:

Delivers the e-mail to the recipient another time.

### Save Message:

Saves the e-mail in the <.msg> file format. You can load this e-mail into another e-mail program.





## Preview of an email

With a double click you can open an selected mail (or with a right click and then select „preview“ from the context menu). Attachments are displayed on the border of the window below and can be opened also with a double click.

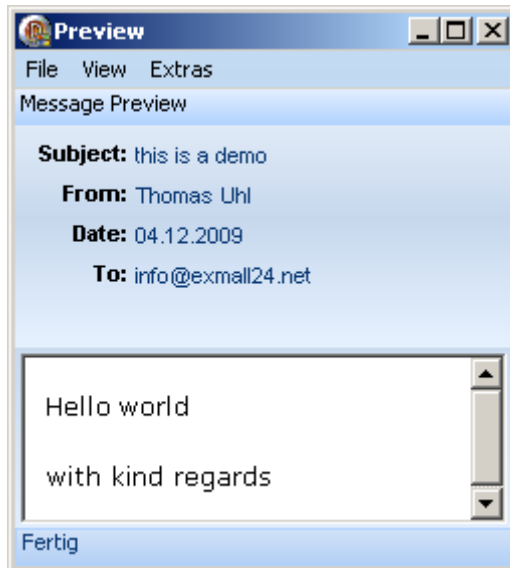


Illustration: E-Mail Preview

In the menu of the preview window you have following options:

**File:** **Close:** Closes the preview window.

**View:** **Message header**

Shows the sending specific header lines of that email. These data can be very helpful for diagnostic purposes. You can examine, when, from whom, to where, how long the mail needs to pass which relay stations.

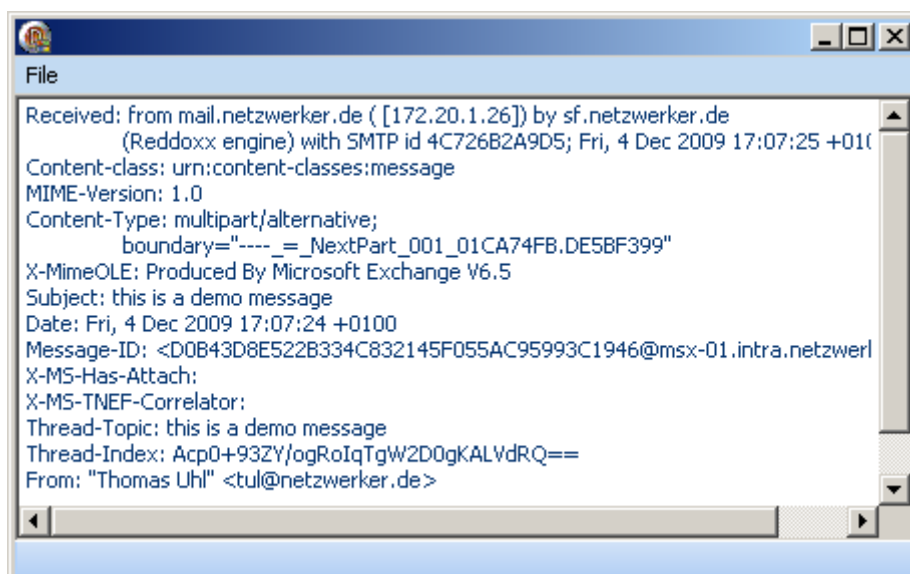


Illustration: Email header data

## Message Source

Shows the complete source code of that email. This means, the header and the body data, independant of the specified content type (PDF, HTML etc.) will be shown in plain text. This can be helpful for diagnostic purposes.

## Extras: Deliver:

You can deliver this email again to your post box..

## Outlook Add-In

### Preview on an email: Within the Outlook-AddIn

With a double click you can open an selected mail (or with a right click and then select „preview“ from the context menu with MS Outlook. Outlook show in the tool bar area its common functions.

Click on “Options” to open the message options windows.



Illustration: E-Mail Vorschau in Outlook

## Options

The Internet header is displayed. See further details as in the section „Previe with the User Console“.

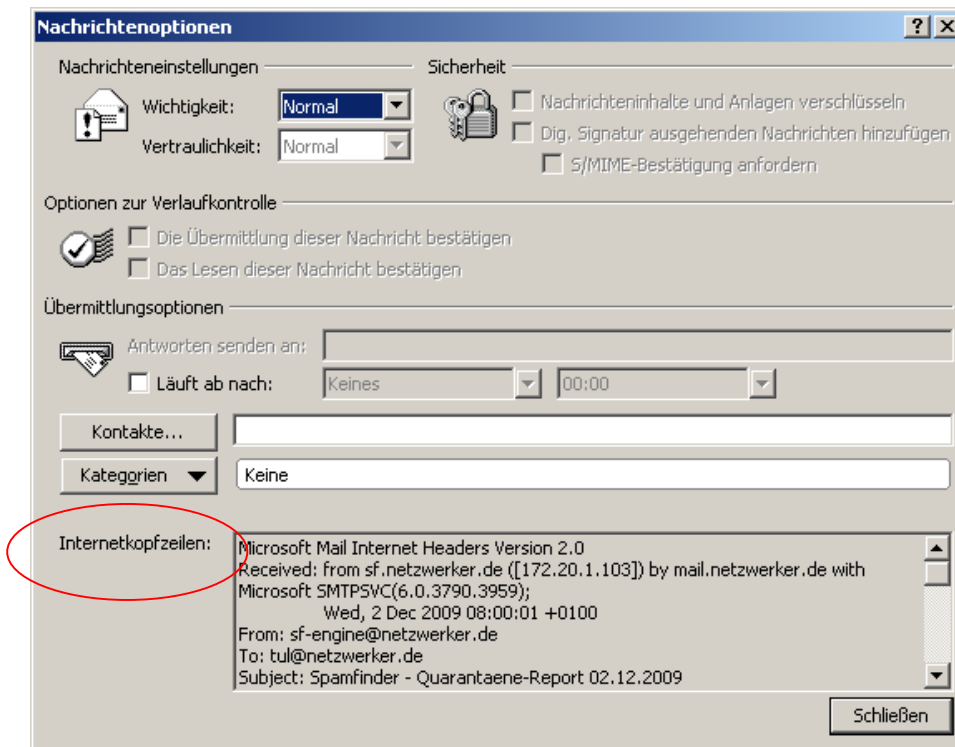


Illustration: Internet Header in an email shown with Outlook

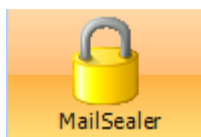
## Message Source

You can view the source code of the message only if you save that message and then open it with an extra editor like notepad or so.

### Deliver:

Exit the message options of Outlook and choose „deliver“ from the archive lists context menu (open with right click) of the selected email.

## 3.5 MailSealer

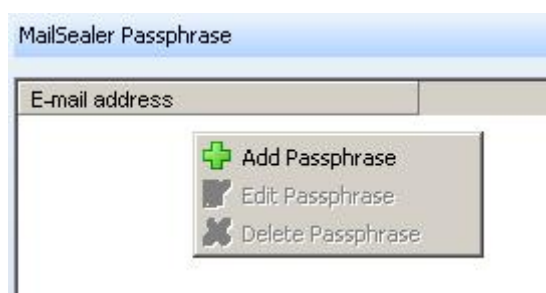


With the integrated REDDOXX MailSealer you can encrypt your e-mails as quickly as simple. To achieve this, very high encryption strength of 256 bit AES is being employed.

### Add a Passphrase

If you would like to encrypt the entire e-mail traffic directed to a specific e-mail address, you proceed as follows:

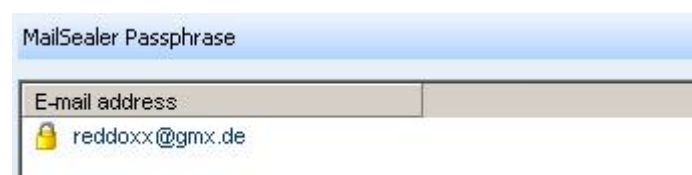
Make a right click in the list. Select 'Add Passphrase' from the context menu.



Specify the respective e-mail addresses and their corresponding passphrases. If you want to apply the encryption immediately, check the 'Active' box.



All e-mails that are being sent to the e-mail address configured will be encrypted automatically.



## Edit Passphrase

In case you want to send future e-mails to a specific address in an unencrypted way again, you proceed as follows:

Make a right click on the e-mail address you want to edit and select the 'Edit Passphrase' option from the context menu.

Clear the 'Active' box and confirm with the 'Save' button.

## 3.6 User Settings



In the User Settings section you can adjust your user profile, your e-mail address, and the settings for your daily queue report and the shape of the Appliance Manager, as well as you can change your password.

## 3.6.1 User Profile

The screenshot shows the 'User Profile' settings interface. At the top, there are three tabs: 'Profile', 'E-Mail Aliases', and 'Filter lists'. The 'Profile' tab is selected. Below the tabs, the 'User Profile' section contains the following settings:

- GUI Theme:** A dropdown menu showing 'Office2007 Blue'.
- Report Language:** A dropdown menu showing 'en'.
- Default Archive display periode:** A numeric input field showing '10' followed by 'days'.
- Enable auto logon:** An unchecked checkbox.
- Use HTML Mail:** A checked checkbox.
- Enable Queue Report:** A checked checkbox.

An 'Apply Settings' button is located below these settings. Below the 'User Profile' section is a 'Change Password' section with three input fields: 'Old password:', 'New password:', and 'Confirm new password:'. A 'Change Password' button is located to the right of these fields.

Image: User Profile Settings

**GUI Theme:** Select a skin for your Appliance Manager

**Report Language:** Select the language for your daily queue report. You can choose between English, German, Italian and Dutch.

**Default Archive display period:**

Initially the archive list shows the e-mails that have been archived within the specified time period. A longer time period can be looked up at any time using the search.

**Enable auto logon:**

You can logon to the Appliance Manager automatically, without typing in your password again. The password is stored on your Appliance.

**Use HTML Mail:**

Check this box if you want to receive the queue report in HTML format.

**Enable Queue Report:**

Check this box if you want to receive the queue report, including a list of spam mails, on a regular basis.

**Change Password:** Here you can change your login password. Specify your old and your new password and click on the '*Change password*' button.

## 3.6.2 E-Mail Aliases

E-mail aliases are e-mail addresses that are assigned to a specific user. This user can manage all e-mail addresses that are assigned to him/her. In the management section you can activate the filtering of spam per e-mail address (default) as well as you can determine a deputy for your e-mail address.



Image: E-Mail Aliases

## Add a new E-Mail Alias

Since the Appliance recognizes new e-mail addresses automatically, usually it is not necessary to add new e-mail aliases manually. If you want to prevent the filtering for a specific e-mail address, you need to add a new e-mail alias manually. If you do not add it manually but wait for the Appliance to recognize the new e-mail address automatically, the filtering of this address will be carried out instantly. To add e-mail aliases manually please proceed as follows:

Make a right click in the free list and select 'Add' from the context menu.

Image: Add E-Mail Alias

## E-Mail address:

Specify the new e-mail address and click on 'Send Request'. You receive an e-mail on this address then.

Image: Verification E-Mail

**Request-ID:** To prevent third parties from managing your new e-mail address, a security check is necessary. Please specify the Verify ID that you can find in the e-mail you have just received from the Appliance, and click on 'Send ID'.

Image: Verification of the new E-Mail Alias using the Verify ID

You can activate or deactivate the filtering of your e-mail alias. Furthermore you can determine deputies, so that other users can manage the queues of this e-mail alias under their account.

Double-click an e-mail alias in the list view to edit it.

Image: Edit E-Mail Alias

**Deputy:** Select a user from the list of deputies who is allowed to manage this e-mail address. The user can then access the spam queue and the archive.

**Profile:** From the *Profile* field you can also select '*No Profile*'. E-mails sent to this address are then not being filtered anymore. After an automatic recreation of an e-mail alias this alias will always be assigned the *Default Profile*.

Click on the 'Save' button to finish editing the settings. The changes are instantly effective.

### 3.6.3 Filter lists

In the filter lists it is possible to set addresses, domains, and subject to trusted and untrustworthy.





Illustration: Filter lists

There are different types of filter lists::

- Address Whitelist: email address is trusted.
- Address Blacklist: email address is untrustworthy.
- Domain Whitelist: email domain is trusted.
- Domain Blacklist: email domain is untrustworthy.
- Subject Whitelist: emails with this subject are trusted.
- Subject Blacklist: emails with this subject are untrustworthy.

You can add, edit and delete whitelist- and blacklist entries.

## Add whitelist

Illustration: Add whitelist

- Email address: Add the email address of a trusted sender.
- Description: A description can be given.

## Add blacklist

Illustration: Add blacklist

Email address:	Add the email address of the sender you want to block.
Description:	A description can be given for this entry.
Action:	Which action should be performed if the above given address matches.

There are 3 types of action:

Quarantine:	The email will be postponed to the quarantine list.
Tag:	The email will be delivered to the recipient with a mark in the subject line.
Decline:	The email will not be accepted from Reddoxx. Therefore a non delivery email is send back.

Valid until:	The validity of this entry is determined.
--------------	---

#### NOTICE

Maintaining the Domain- and subject filter lists goes in the same matter.

## 3.7 Logoff



By clicking on the 'Logoff' symbol the connection to the Appliance will be interrupted. The Login window appears so that you can login again, also with another username.



## 4 The Reddoxx Outlook AddIn

The Reddoxx Outlook AddIn integrates the Reddoxx user console into MS Outlook. It gets launched with the start of MS Outlook. The main difference to the user console or the web interface is mainly the ability to archive mails from your mail box into the central Reddoxx Mail Archive. Furthermore there is a feature to add a spam sender onto the blacklist. Most of the feature set equals to the functions of the user console.

### NOTICE

The Reddoxx Outlook AddIn is supports only MS Outlook. Other mail clients such as Outlook Express, Lotus Notes or Thunderbird are not supported.

## 4.1 Installation of the Outlook AddIn

1. **Download** the setup file of the under the URL  
<http://support.reddoxx.net/downloads.php>
2. **Launch** the setup with a double click onto the <.msi> file. A welcome screen appears.

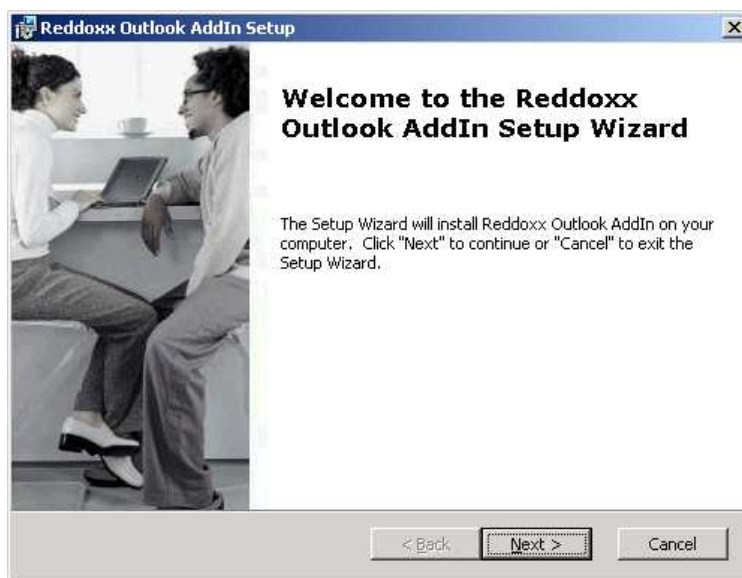


Illustration: Setup Welcome screen

3. Continue with „**Next**“.

### NOTICE

Note that MS Outlook must be closed completely before this setup. Make sure that the MS Outlook process is not listed in the task managers process bar.

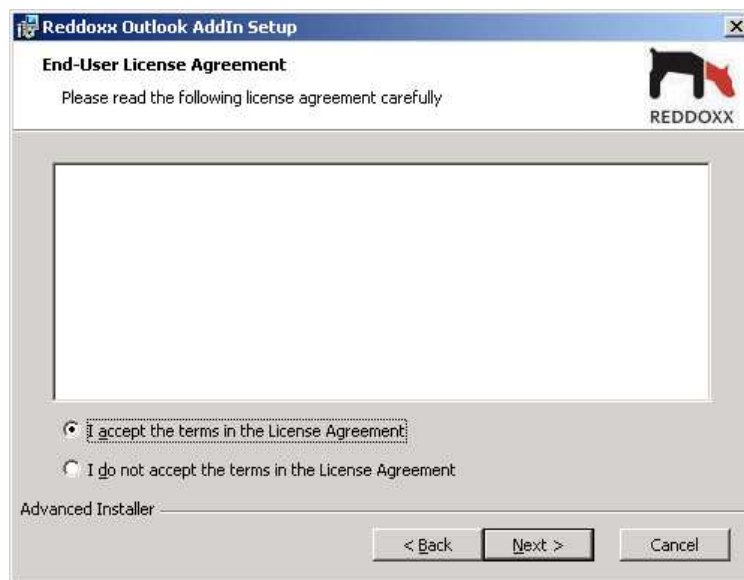


Illustration: License agreement

4. Read the end user license agreement and click on „**Next**“ if you agree to them.



Illustration: Installation folder

5. Choose an installation folder of your choice and continue with „**Next**“.



Illustration: Installation ready

6. The Setup wizard is ready to install. Click on „Install“ to start the installation now.

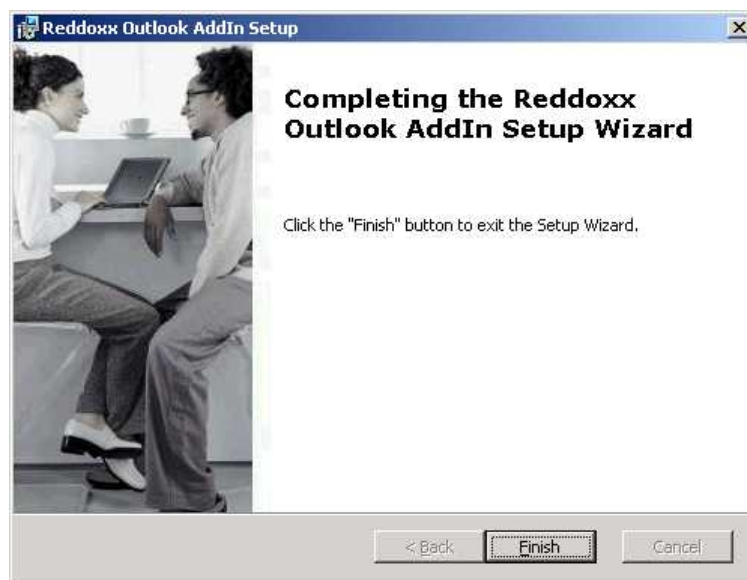


Illustration: Installation finished

7. The installation now is finished. Click on „**Finish**“ to exit the setup.

You can now launch MS Outlook.

## 4.2 Outlook menu overview

After launching MS Outlook a Reddoxx button appears in the symbol bar. Additionally you can see in your mail box tree a new folder named Reddoxx Outlook AddIn.



Illustration: Reddoxx Logon Button

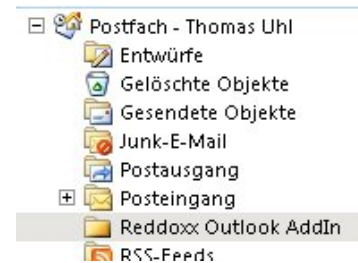


Illustration: Reddoxx Folder

With a click onto the Reddoxx button or a click onto the Reddoxx folder the login screen appears.

## 4.3 Reddoxx logon

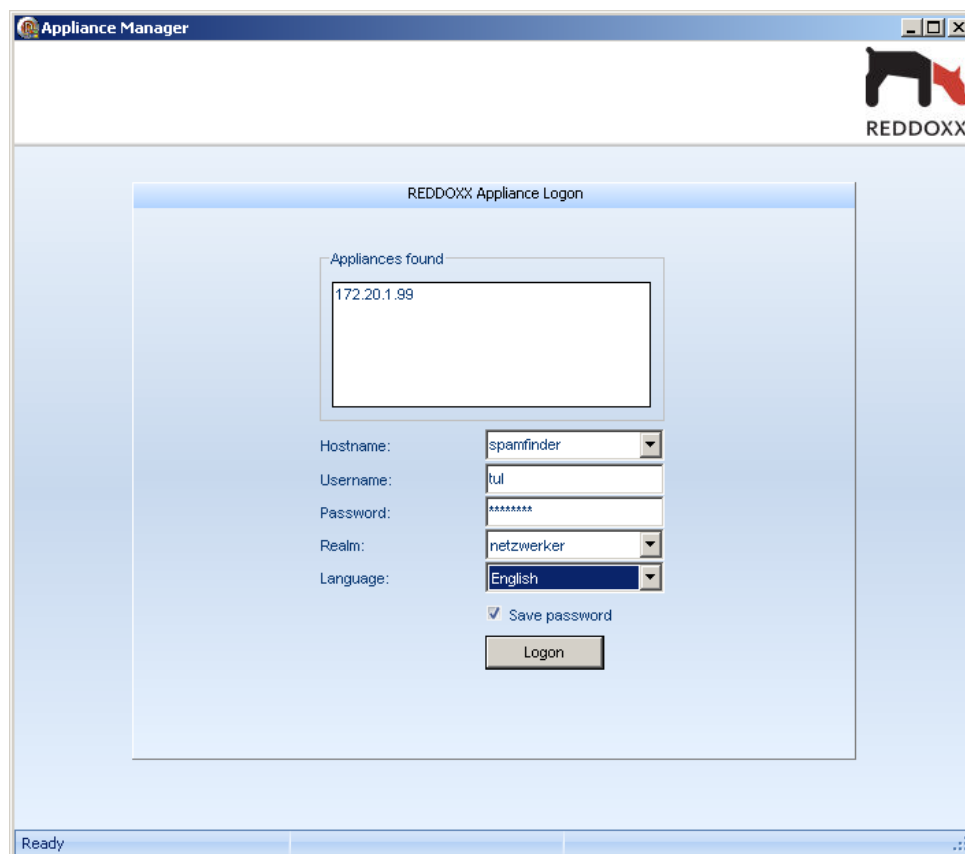


Illustration: Logon screen

**NOTICE**

The logon process equals to the User console described in chapter 2.

## 4.4 The Reddoux menu

The design of the menu is very close to the user console. The only difference is that the menu items are shown horizontally, instead of upright.

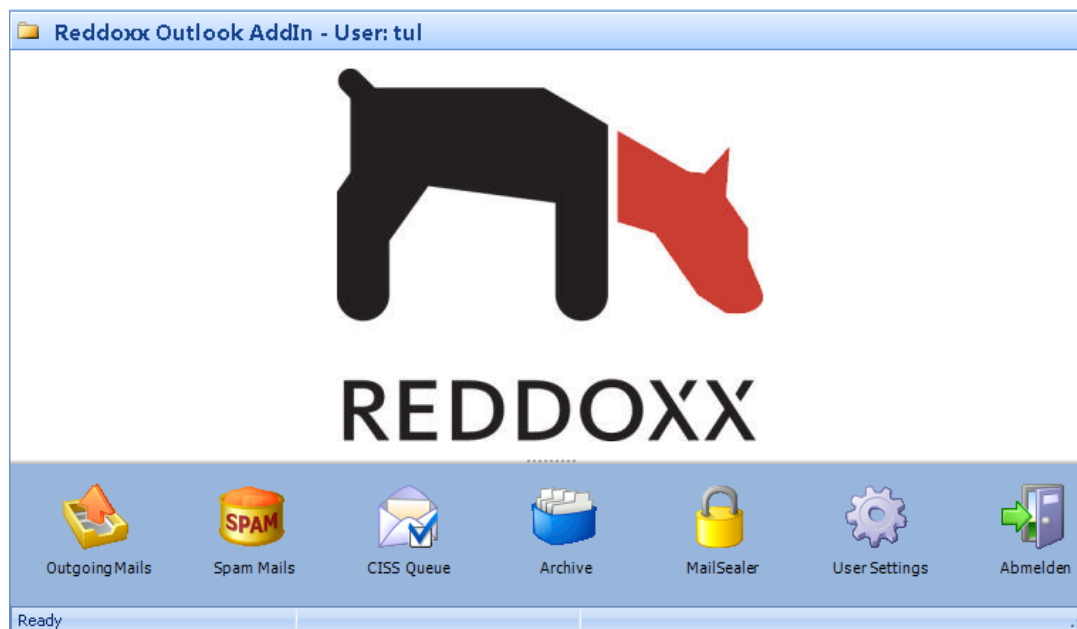


Illustration: Welcome screen with menu items

**HINWEIS**

The menu items equals to the user console described in chapter 3.

## 4.5 Message archiving

You can post archive emails or a complete folder from your mail box into the Reddoux Appliance.

1. Login to your Reddoux Appliance.
2. Select your email from your mail box and folder you wish to archive.

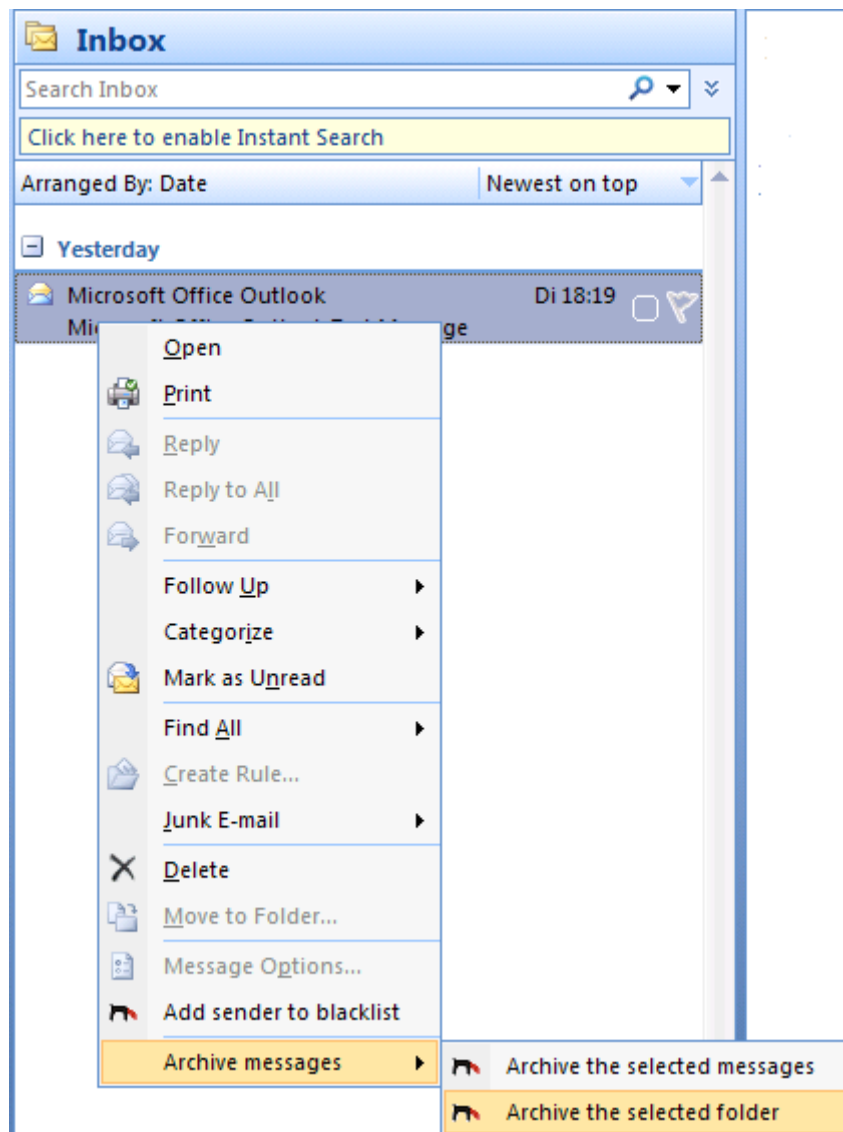


Illustration: Nachricht archivieren

3. Right click to the message you want to archive. The context menu opens and show following options:
  - Archive the selected message
  - Archive the selected folder

#### NOTICE

If you choose „archive folder“ each single mail inside the selected folder will be listed in the archive window. Consider this if you are playing with thousands of messages that this can take some time. All other options are the same as for “archive message”.

Before the archiving process starts, all selected emails are listed.



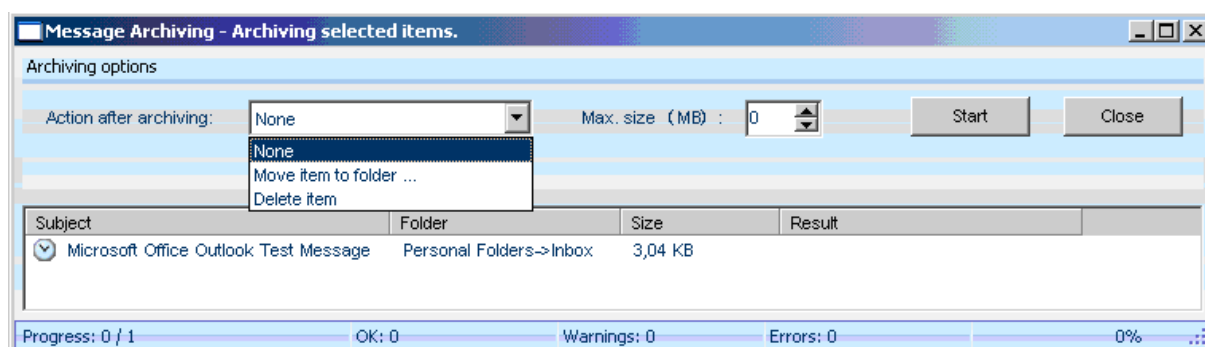


Illustration: Archive messages window

You have the choice of following options in the archiving window.

### Action after archiving:

- Move item to folder:** After archiving is finished the folder gets moved to the specified folder.
- Delete item:** The message gets deleted after archiving has finished.
- None:** There is no any action after archiving.

### Max. size (MB):

The size limit in mega bytes of a single message until it gets archived.

### Start:

Starts the archiving process.

### Close:

Closes the archiving window.

During archiving you can watch the progress bar.



Illustration: Archiving messages dialog with progress bar

## 4.6 Blacklisting an email manually

If an email was not filtered by the appliance, you can set the email sender address onto the appliance's blacklist.

1. Select the email and click right.

The context menu opens.

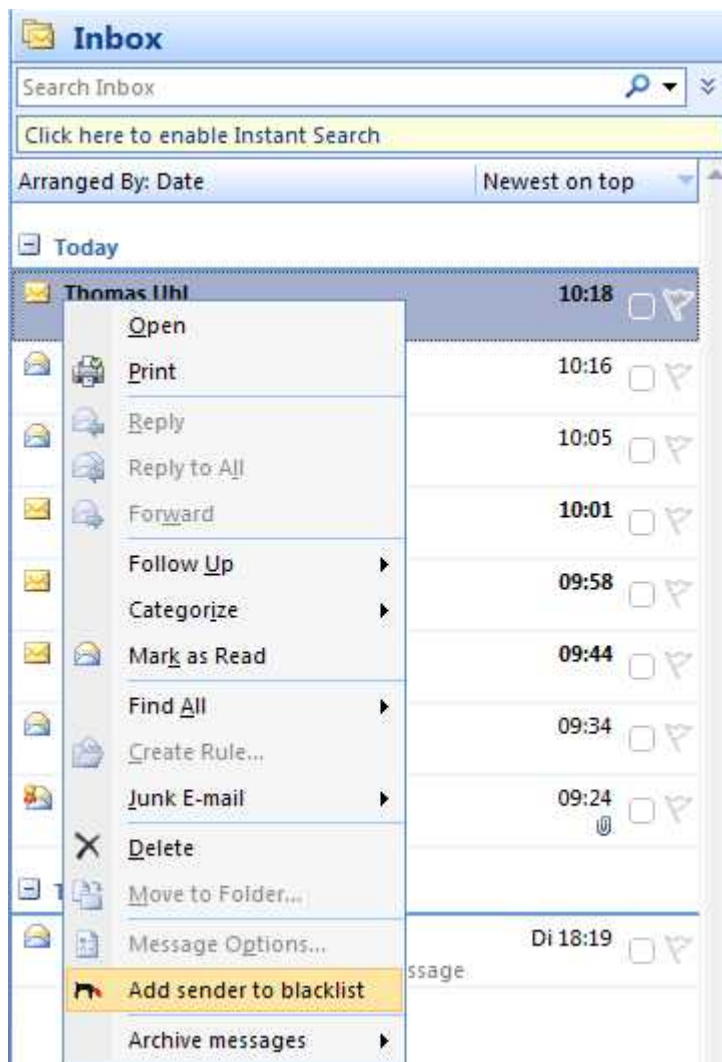


Illustration: Add the sender's address to the blacklist

2. Click on „Add sender to blacklist“.

The sender of this selected email is shown in a new window for confirmation.

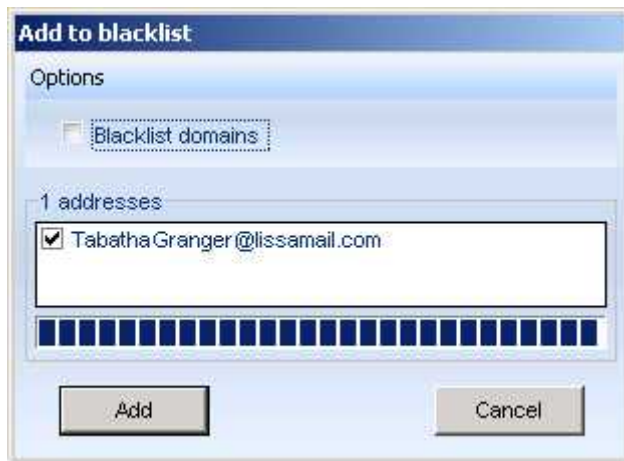


Illustration: Adding the sender to the blacklist

### 3. Blacklist domains:

You also can block the complete domain if this option is enabled by the appliance policies. Contact your administrator if you need to have this feature enabled.

### 4. Click on „Add“.

The sender now is added to the blacklist. The window closes.

## 5 Glossary

### A

**ABL Filter:**

Address blacklist filter – checking the sender address against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. The lists are maintained manually by the administrator or the user.

**Advanced RBL Filter:**

Advanced Realtime Blacklist Filter - All email servers involved in the transport of the incoming mail are checked against public blacklist servers. We do not assume any guarantee for the function of the selected blacklist servers as well as the absence of errors in the list entries on the blacklist servers.

**Appliance:**

The appliance is the hardware component of the Spamfinder - the REDDOXX Appliance. There are three variants of the REDDOXX Appliance. This ensures that the demands of all sizes of companies and email traffic are covered optimally. Observe the warning and safety notices!

**AWL Filter:**

Domain whitelist filter – checking the sender address against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. Some filters establish this list automatically. The lists are further maintained manually by the administrator or the user.

### B

**Bayes Filter:**

Via the content check, the Bayes filter determines the spam probability. Spamfinder automatically establishes the word lists. We do not assume any liability for wrong detection.

### C

**CISS:**

Confirmation Interactive Site Server, in short CISS, is a unique, several stage control process, which ensures the permanent exchange of wanted mails between sender and receiver. Intelligent authorization of the sender by means of CISS (registered for patent), a unique challenge/response-functionality.

**CISS Filter:**

Confirmation Interactive Site Filter – This method ensures that the sender is a natural person. For this purpose, a corresponding Internet page is provided via the Spamfinder portal, which is accessible in the Internet. The availability of the Spamfinder portal is at least 98.5% per year.

**Cluster:**

A cluster denotes a number of networked computers. These networked computers are available for parallel processing. Partial tasks belonging to a task are processed. Contrary to parallel computers, the load distribution takes place on the level of individual processes started on one or several machines in the cluster. You therefore do not require parallel software or special operating systems but instead a scheduler that assigns the partial tasks to the individual computers. Alternatively, clusters are also used to increase the availability of systems.

**Console:**

Software component the REDDOXX Appliance is controlled by.

## D

**DBL Filter:**

Domain blacklist filter – checking the sender domain against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. The lists are maintained manually by the administrator or the user.

**DMZ:**

A DMZ means demilitarized zone. A DMZ is an intermediate network that is formed at network interfaces but does not belong to either of the networks. It represents an inherent network that is not as heavily secured as the network that is actually to be protected. With simple security gateways, DMZ is usually generated at a third interface of the package filter. If the security gateway consists of a package filter - application level gateway - package filter, another interface of the application level gateway (ALG) usually serves as DMZ interface. If package filters or ALG have more than three interfaces, additional DMZ can be formed.

**DNS:**

The Domain Name System (DNS) is one of the most important services in the Internet. The DNS is a distributed database that manages the name space in the Internet.

**Domain:**

A domain is a coherent section of the hierarchic DNS name space. Starting from its domain name, a domain always comprises the entire subordinate tree structure.

**DWL Filter:**

Domain whitelist filter – authorizing the sender domain against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. The lists are maintained manually by the administrator or the user.

## F

**Failover:**

A failover denotes a technology in the IT sector that serves to keep data and services highly available.

## H

**Host name:**

The host name of the REDDOXX Appliance in the network.

## L

### **LDAP:**

LDAP (Lightweight Directory Access Protocol) is a network protocol applied for so-called directories. It handles the communication between the LDAP client (e.g. with a mail server or a digital address book) and the directory server. It offers all log-specific functions required for such communication: registration on the server, the search query and data modification.

## M

### **Mail Hop:**

Mail hop is when an email is transferred from one server to another. Each of these servers is regarded as a mail hop.

## N

### **NBL Filter:**

Network blacklist filter - Checking the IP address of the email server against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. The lists are maintained manually by the administrator or the user.

### **NWL Filter:**

Network whitelist filter - Authorization of the IP address of the email server against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. The lists are maintained manually by the administrator or the user.

## O

### **OS:**

Operating System.

## Q

### **Quarantine:**

For all authorized users, the REDDOXX Appliance contains quarantine mailboxes, which can be set up individually. Together with the achieved false positive rates, this feature enables you to achieve the conformity with the valid laws.

## R

### **RAID:**

A RAID system (Redundant Array of Inexpensive Disks, often also Redundant Array of Independent Disks) serves to organize several physical hard disks of a computer to form a powerful and safe logical drive.

### **RBL Filter:**

**Realtime Blacklist Filter** - The sending email servers are checked against public blacklist servers. We do not assume any guarantee for the function of the selected blacklist servers as well as the absence of errors in the list entries on the blacklist servers.

#### **Realm:**

A realm is a section similar to a domain where you authenticate yourself. (Also see the chapter: "User Administration - Login Configuration")

#### **RVC Filter:**

**Recipient Verify Check Filter** - To protect the local email server from "spam floods", the recipient address is checked by asking the respective email server, whether the recipient is known. This function is currently available for Microsoft Exchange Server as of version 5.5.

## **S**

#### **SBL Filter:**

**Subject Blacklist Filter** – Checking the email subject against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. The lists are maintained manually by the administrator or the user.

#### **SMTP:**

**Simple Mail Transfer Protocol**. This protocol enables you to fit out an email with a bit more than just sending it "as is"! The protocol has several function options. On the one hand, SMTP lets your emails go straight to the receiver and on the other hand SMTP enables routing your emails via different servers, so-called MTA, to the recipient. Almost all email clients use this protocol to send electronic mail.

#### **SRC Filter:**

**Sender Receive Check Filter** - Checks whether the sender would also accept an email. Wrong detection, e.g. with newsletters or other automatically generated emails, cannot be ruled out, but prevented by making the respective entries in the positive lists.

#### **SWL Filter:**

**Subject Whitelist Filter** – Authorization of the email subject against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. The lists are maintained manually by the administrator or the user.

## **T**

#### **TCP/IP:**

**Transmission Control Protocol / Internet Protocol**. TCP/IP is the protocol that controls the connections/data exchange between computers in the Internet. When transmitting information, TCP divides the sent data into small packages, gives them a check sum (transmission safety) and numbers them consecutively (to ensure that the packages are reassembled again in the correct sequence). The TCP packages also contain the addresses of sender and receiver (IP addresses).

## **V**

#### **Virus Scanner:**

The virus scanner checks the attachments of all emails for viruses. Packed files are temporarily unpacked and checked. Emails in which a virus was detected are saved in a quarantine section. Only the administrator has access to this section. Your Spamfinder obtains the virus signatures directly from the scanner manufacturer (ClamAV). We do not assume any guarantee for the topicality of the signature files as well as the availability of the signature server. We do not assume any liability for damage caused by undetected viruses.